UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/364,835	07/30/1999	BAIJU V. PATEL	INTL-0182-US	9974

7590 08/09/2005

TIMOTHY N TROP
TROP PRUNER HU & MILES PC
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/364,835	PATEL ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,13-20 and 28-37* is/are pending in the application.

4a) Of the above claim(s) *6-12 and 21-27* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,13-20 and 28-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Corrected

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7, 13-20, and 28-37 have been are pending.

Applicant has amended claims 1 and 16.

Applicant has cancelled claims 8-12 and 21-27.

2. Claims 1-7, 13-20, and 28-37 remain rejected. This is a Final rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-7, 16-20, and 27-37 are rejected under 35 U.S.C. 102(b) as being anticipated by Caputo, et al. (US 5,546,463).

As per claim 1:

Caputo discloses a method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block; **[col.6, lines 18-21; security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo determines the verification process based on the algorithm chosen to implement.]**

generating security information to pass along with the data block, the security information identifying the security service; and **[see col.6, lines 1-18; the security information is the type of algorithm chosen for encryption/decryption or authentication algorithm to authenticate the data communicated and necessary for the recipient to verify in the verification process]**

using a computer peripheral device adapted to control communication with the communications channel **[see col.4, lines 24-44]** to select the security service from other security services based on the security information; and **[col.5, lines 48-67 and col.8, lines 59-67]**

processing, in a computer peripheral device, the data block according to the security information; **[see col.6, lines 22-35]**

As per claim 2: see col.6, lines 22-35; discusses performing cryptographic processing of the data block.

As per claim 3: see col. 8, lines 47-54; discusses receiving the data block from a software routine and routing the processed data block back to the software routine after processing.

As per claim 4: see col.6, lines 18-51; discloses determining if the security service can be performed by the computer peripheral device and if not, processing the data block according to the security service in a software routine instead of the computer peripheral device **[see col.8, lines 47-54]**.

As per claim 5: see col.8, lines 11-16 and col.9, lines 21-22; discussing the Internet Protocol Security.

As per claim 16:

Caputo discusses a controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data **[see col.5, lines 11-15 and col.8, lines 10-16]** and associated security control information, the security control information **[see col.6, lines 1-18; the security information is the type of algorithm chosen for encryption/decryption or authentication algorithm to authenticate the data communicated and necessary for the recipient to verify in the verification process]** identifying a security service to be performed on the data; and **[col.6, lines 18-21 and col.8, lines 11-16; security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data**

block. Caputo determines the verification process based on the algorithm chosen to implement.]

a cryptographic engine **[see col.2, lines 20-63 and col.5, lines 17-24]** to select the security service from other security services based on the security control information **[col.5, lines 48-67]** and cryptographically processes the data selection, the cryptographic engine being in the computer peripheral device. **[see col.6, lines 22-35 and col.8, lines 59-67]**

As per claim 17:

Caputo discusses the storage device containing information identifying security services to be performed **(see col.6, lines 18-21 and col.8, lines 11-16)**, the received security control information selecting a portion of the security services information in the storage device **(col.5, lines 48-67)**, wherein the cryptographic engine processes the data according to the selected portion of the security services information. **(see col.6, lines 22-35 and col.8, lines 59-67)**

As per claim 18: see col.5, lines 45-67 and col.7, lines 20-25; discussing a device adapted to change the contents of the storage device to update the security services information. **[it is inherent in the art that updating to make sure the system doesn't have outdated or unnecessary data and updating inherently helps the security of a system operate more efficiently.]**

As per claim 19: see col.5, lines 45-67 and col.8, lines 11-16; discussing a device adapted the security services information based on a predetermined replacement policy. **[it is inherent in the art that a replacement policy ensures the system doesn't have outdated or unnecessary data that would cause the system to slow down or takes longer period of time to process and because a replacement policy inherently further helps the security of a system.]**

As per claim 20: see col.6, lines 1-36 and col.8, lines 11-16; discussing the security services information includes security association information.

As per claim 28:

Caputo discloses a method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block; **[col.6, lines 18-21 and col.8, lines 11-16; security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo determines the verification process based on the algorithm chosen to implement.]**

generating security information to pass along with the data block **[see col.6, lines 1-18; the security information is the type of algorithm chosen for encryption/decryption or authentication algorithm to authenticate the data communicated and necessary for the recipient to verify in the verification process]**, the security information identifying at

least one of an encryption algorithm **[see col.5, lines 45-50]** and an authentication algorithm **[see col.6, lines 7-16]** to be performed by the security service; and **[see col.4, lines 30-44]**

processing, in a computer peripheral device adapted to control communication with the communications channel **[see col.4, lines 24-44]**, the data block according to the security information. **[see col.6, lines 18-35 and col.8, lines 59-67]**

As per claim 29: see col.5, lines 21-23; discusses the processing includes performing cryptographic processing of the data block.

As per claim 30: see col. 8, lines 47-54; discusses receiving the data block from a software routine and routing the processed data block back to the software routine after processing.

As per claim 31: see col.6, lines 18-51; discloses determining if the security service can be performed by the computer peripheral device and if not, processing the data block according to the security service in a software routine instead of the computer peripheral device. **[see col.8, lines 47-54]**

As per claim 32: see col.8, lines 11-16 and col.9, lines 21-22; discusses identifying a security service according to an Internet Protocol security protocol.

As per claim 33:

Caputo discloses a controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data **[see col.5, lines 11-15 and col.8, lines 10-16]** and associated security control information **[see col.6, lines 1-18; the security information is the type of algorithm chosen for encryption/decryption or authentication algorithm to authenticate the data communicated and necessary for the recipient to verify in the verification process]**, the security control information identifying at least one of an encryption algorithm **[see col.5, lines 45-50]** and an authentication algorithm **[see col.6, lines 7-16]** to be performed on the data; and **[see col.4, lines 30-44]**

a cryptographic engine to cryptographically process the data based on the security control information **[see col.6, lines 18-35 and col.8, lines 59-67]**, the cryptographic engine being a computer peripheral device. **[col.5, lines 16-29]**

As per claim 34: see col.5, lines 19-20 and 48-50; discusses a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.

As per claim 35: see col.5, lines 45-67 and col.7, lines 20-25; discusses a device adapted to change the contents of the storage device to update the security services information. **[it is inherent in the art that updating to make sure the system doesn't have outdated or unnecessary data and updating inherently helps the security of a system and to operate more efficiently]**

As per claim 36: see col.5, lines 45-67 and col.8, lines 11-16; discusses the device is adapted to update the security services information based on a predetermined replacement policy. **[it is inherent in the art that a replacement policy to makes sure the system doesn't have outdated or unnecessary data that would cause the system to slow down or takes longer period of time to process and because a replacement policy inherently further helps the security of a system]**

As per claim 37: see col.5, lines 44-50 and col.6, lines 7-16 ; discusses the security services information includes security association information.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 13-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Abadi, Et Al. (US 5,268,962).

As per claim 13:

Abadi discloses an article including a machine-readable storage medium containing instructions for execution in a system including a computer peripheral device adapted to control communication with a communications channel, the instructions when executed causing the system to: **(see FIG.3)**

receive a data block from the computer peripheral device; **(see col.5, lines 52-55)**

determine from information in the data block if a security service has not been performed on the data block by the computer peripheral device; and **[see col.3, lines 61-65 and col.4, lines 24-27; security service is the type of security rendered for the data packet prior to transmitting the packet to the host/destination. Abadi determines the security measure needed for the packet according to the other host by identifying**

the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet.]

process the data block if the security service has not been performed on the data block by the computer peripheral device. **[See col.4, lines 30-31 and col.6, lines 67-68; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface and cryptographic processing is the process of encryption or decryption.]**

As per claim 14: see col.7, line 63 – col.9, line 3; discussing the instructions causing the system to retrieve security information associated with the data block and sent the data block and security information to the computer peripheral device to perform the security service.

As per claim 15: see col.6, lines 7-63; discussing the instructions causing the system to perform the security service on the data block.

Response to Arguments

5. Applicant's arguments with respect to claims 1 and 16 have been considered but are moot in view of the new ground(s) of rejection.

The examiner finds Caputo, et al to teach the limitations of amended claims 1 and 16. Claims 1-5 and 16-20 are final necessitated by new grounds of rejection.

6. Applicant's arguments filed 5/16/2005 have been fully considered but they are not persuasive.

Claims 13-15 and 28-37 was not amended and the examiner maintains the rejection with the same prior art, Abadi, et al.

Claims 13-15 remains rejected by Abadi. Abadi discloses determining from the BQI value in the packet if a security service has been performed by comparing to the record if there is a match and if the BQI value is invalid, the host can still handle the packet **[see col.6, lines 8-23]**. Once compared and matched to the record, BQI value then leads to generating a decryption key for decrypting the encrypted portion of the received packet **[see col.6, lines 25-36]**. The examiner gives the broadest reasonable interpretation for the limitation of claim 13, lines 6-9. On lines 6-7, the BQI value is the information that determines whether a security service was performed by reading the header of each of the received data packet in order to process the BQI value and to generate

the decryption key **[see col.5, lines 57-60 and col.6, lines 25-26]**. For lines 8-9, the examiner broadly interprets to process the data if security service has not been performed where Abadi teaches that even if the BQI does not match, then the packet can still be processed **[see col.6, lines 22-23]**. Abadi determines whether to process the packets with invalid BQI values, therefore does teach having the capability to process the data if security has not been performed.

Claims 28-37 remains rejected by Caputo, et al., because Caputo does teach security information contained with the data block or in the message where this information is the type of algorithm that may contain a key chosen for encryption/decryption or a digital signature for authentication to authenticate the message transmitted and necessary for the recipient to verify in the verification process **[see col.6, lines 1-20]**. Caputo disclose the security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo is able to select a security service by choosing from a variety of cryptographic algorithms **[col.5, lines 45-50]** and determine the verification process based on the algorithm chosen to implement **[col.6, lines 18-21]**.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859.

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXA[illegible]
TECHNOLOGY CENTER 2100